# Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state

Chuan Wang[1], Fu Guo Deng[3] and Gui Lu Long[1,2]
[1] *Department of Physics and Key Laboratory For Quantum Information and Measurements, Tsinghua University, Beijing 100084, People's Republic of China*
[2] *Key Laboratory for Atomic and Molecular Nanosciences, Tsinghua University, Beijing 100084, People's Republic of China*
[3] *The Key Laboratory of Beam Technology and Materials Modification of Ministry of Education, and Institute of Low Energy Nuclear Physics, Beijing Normal University, Beijing 100875, People's Republic of China*
(Dated: February 1, 2008)

A multi-step quantum secure direct communication protocol using blocks of multi-particle maximally entangled state is proposed. In this protocol, the particles in a Green-Horne-Zeilinger state are sent from Alice to Bob in batches in several steps. It has the advantage of high efficiency and high source capacity.

PACS numbers: 03.67.Dd,03.67.Hk,03.67.-a



Quantum communication becomes one of the most important applications of quantum mechanics today. Quantum key distribution(QKD) is one of the most mature techniques, providing a secure way for creating a private key with which two authorized parties, Alice and Bob, can realize secure communication. QKD has attracted a widespread attention and progressed quickly [1, 2, 3, 4, 5, 6] over the past two decades.

Recently, a new concept in quantum cryptography, quantum secure direct communication (QSDC) was proposed. Upto date, QSDC has been studied by many groups [7, 8, 9, 10, 11, 12, 13, 14, 15]. With QSDC Alice and Bob can exchange the secret message directly without generating a private key first and then encrypting the secret message and then send the ciphertext through classical communication. The QSDC protocol originally proposed by Beige et al. [7] is only a scheme for transmitting secret information which can be read out with an additional classical information for each qubit. Later, Boström and Felbinger put forward a ping-pong QSDC scheme following the idea of quantum dense coding [4] with Einstein-Podolsky-Rosen (EPR) pairs. As pointed out by their authors, ping-pong protocol is just a quasi-secure direct communication protocol as it leaks some of the secret message in a noisy channel. In Ref. [9], some of us proposed a two-step QSDC protocol using entangled particles. In this paper, the idea of transmitting quantum data in blocks for the security of QSDC was proposed.

Recently, Gao et al. [16] designed a protocol for controlled quantum teleportation and secure direct communication using GHZ state.

As GHZ-state has a larger Hilbert space, protocols based on them can provide larger source capacity. With the development of technology, the generation and manipulation are becoming more sophisticated, and practical applications of these highly entangled objects are expected in the future. It is thus interesting to look for ways of using these quantum objects in quantum key distribution. In this paper, we present a QSDC protocol using maximally entangled three-particle Green-Horne-Zeilinger(GHZ) states. It will be shown that this QSDC protocol appears to provide better security. In addition, this QSDC protocol can also be equipped with quantum privacy amplification so that it can work under realistic environment.

We first introduce the idea of GHZ state dense coding briefly. Dense coding using three particle entangled states has been proposed by Lee et al. [17]. The protocol we propose is the application of three particle dense coding to QKD. Suppose the maximally entangled three-particle state is

$$|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle_{ABC} + |111\rangle_{ABC}). \qquad (1)$$

There are eight independent GHZ-states, namely

$$\begin{aligned}
|\Psi\rangle_1 &= \tfrac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \ |\Psi\rangle_2 = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle);\\
|\Psi\rangle_3 &= \tfrac{1}{\sqrt{2}}(|100\rangle + |011\rangle), \ |\Psi\rangle_4 = \frac{1}{\sqrt{2}}(|100\rangle - |011\rangle);\\
|\Psi\rangle_5 &= \tfrac{1}{\sqrt{2}}(|010\rangle + |101\rangle), \ |\Psi\rangle_6 = \frac{1}{\sqrt{2}}(|010\rangle - |101\rangle);\\
|\Psi\rangle_7 &= \tfrac{1}{\sqrt{2}}(|110\rangle + |001\rangle), \ |\Psi\rangle_8 = \frac{1}{\sqrt{2}}(|110\rangle - |001\rangle)
\end{aligned} \qquad (2)$$

By performing single-particle unitary operations on any two of the three particles, one can change from one GHZ-state to another. The unitary operations are the product of the Pauli and identity matrices: $I, \sigma_x, i\sigma_y, \sigma_z$. Though there are altogether 16 such operations, only half of them can generate distinguishable states. For our purpose, we choose the following eight operations

$$\begin{aligned}
U_1 &= \sigma_z \otimes \sigma_z, \ \ U_2 = I \otimes \sigma_z;\\
U_3 &= i\sigma_y \otimes \sigma_z, \ \ U_4 = \sigma_x \otimes \sigma_z;\\
U_5 &= I \otimes \sigma_x, \ \ U_6 = \sigma_z \otimes \sigma_x;\\
U_7 &= \sigma_x \otimes \sigma_x, \ \ U_8 = i\sigma_y \otimes \sigma_x,
\end{aligned} \qquad (3)$$

to realize the following transformation,

$$U_k|\Psi\rangle_1 = |\Psi\rangle_k, k = 1, 2, ..., 8. \quad (4)$$

Starting from the state $|\Psi\rangle_1$, one can match each unitary operation with a GHZ-state uniquely.

We now describe the multi-step quantum secure direct communication using GHZ state in detail. First Alice and Bob make an agreement that each of the states $|\Psi\rangle_k$ represents a three bits binary number, namely $|\Psi\rangle_1 \Longrightarrow 000$, $|\Psi\rangle_2 \Longrightarrow 001$, $|\Psi\rangle_3 \Longrightarrow 010$, $|\Psi\rangle_4 \Longrightarrow 011$, $|\Psi\rangle_5 \Longrightarrow 100$, $|\Psi\rangle_6 \Longrightarrow 101$, $|\Psi\rangle_7 \Longrightarrow 110$, $|\Psi\rangle_8 \Longrightarrow 111$ respectively. Then the specific steps in the QSDC protocol is

Step 1: Alice produces a sequence of $N$ GHZ states. Each GHZ-state is in state

$$|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle_{ABC} + |111\rangle_{ABC}). \quad (5)$$

We represent the sequence of $N$ GHZ-states as $[P_1(A)P_1(B)P_1(C),\ P_2(A)P_2(B)P_2(C),\ ...,\ P_N(A)P_N(B)P_N(C)]$, where the numbers in the subscript is the order number of the GHZ-triplet, and the alphabets inside the bracket, $A$, $B$ and $C$ , represent the particles within each GHZ-triplet.

Step 2: Alice takes the $C$-particle from each GHZ triplet (particle $P_M(C)$, $M = 1, 2, ..., N$) to form a $C$-sequence, $[P_1(C), P_2(C),...\ P_N(C)]$. Then she sends the $C$-sequence to Bob as shown in Fig 1.

Step 3: When Bob receives the $C$-sequence $[P_1(C), P_2(C),...\ P_N(C)]$. Alice and Bob perform a security check to see if there is eavesdropping in the line. Security check can be realized by some measurements so that the entangled states collapse. Here we provide two alternatives.

*Method 1 contains the following steps.* First, Bob randomly chooses particles from his $C$-sequence to make either $\sigma_z$ or $\sigma_x$ measurement. This collapses the GHZ state into either $|000\rangle$ or $|111\rangle$ with equal probability if $\sigma_z$ is measured, or into $(|+x+x\rangle + |-x-x\rangle)/\sqrt{2}$ if $|+x\rangle$ is obtained, $(|+x-x\rangle + |-x+x\rangle)/\sqrt{2}$ if $|-x\rangle$ is obtained when $\sigma_x$ is measured. Then he announces the positions of these particles and the kind of measurement he has made. With this information, Alice can make a $\sigma_z$ measurement on the two particles in the corresponding GHZ-triplet if Bob measures $\sigma_z$, or a $\sigma_x$ measurement on the two particles in the corresponding GHZ-triplet if Bob measures $\sigma_x$. They check the results to discover the existence of Eve. If the channel is safe, the results must be completely correlated, i.e. if Bob get $|0\rangle(|1\rangle)$, then Alice get $|00\rangle(|11\rangle)$ when they choose their measurements along z-direction, and similar case happens for the $\sigma_x$. For instance, if Eve gets hold the $C$ particle and sends a fake $C'$ particle to Bob, this security check will discover her.

*Method 2 contains the following steps.* First, Bob randomly chooses particles from his $C$-sequence and he also measures each of these chosen particles using either $\sigma_z$ or $\sigma_x$. This collapses the GHZ state into either $|000\rangle$ or $|111\rangle$ with equal probability if $\sigma_z$ is measured, or into $(|00\rangle + |11\rangle)/\sqrt{2}$ if $|+x\rangle$ is obtained, $(|00\rangle - |11\rangle)/\sqrt{2}$ if $|-x\rangle$ is obtained when $\sigma_x$ is measured. Then he announces the positions of these particles and the kind of measurement he has made. With this information, Alice can make a $\sigma_z$ measurement on the two particles in the corresponding GHZ-triplet if Bob measures $\sigma_z$, or a Bell-basis measurement if Bob measures $\sigma_x$. They then publish their measured result to check the existence of Eve. If the channel is safe, the results must be completely in accordance. On the condition of safe channel, they go to the next step, otherwise they stop the communication.

Step 4: Alice encodes her information on the remaining two qubits message sequence, or the $AB$-sequence, $[P_1(A)P_1(B),\ P_2(A)P_2(B),\ ...,\ P_N(A)P_N(B)]$ by performing the unitary operations, which has been described by equations (3) and (4). For the secure communication, Alice selects some sampling pairs of her particles, randomly chosen from the $AB$-sequence and performs one of the eight operations randomly on them. The remaining pairs of particles in the $AB$-sequence are encoded with secret messages. After that she sends the second block of particles $[P_1(B),\ P_2(B),...\ P_N(B)]$ which is formed by the $B$ particles of the GHZ state to Bob. After Bob receives these $B$ particles, they make a security check in which Alice starts the security check by choosing some of the sampling pairs for measurement using one of the checking method described in step 3. If the security check is passed, Alice then sends Bob the last sequence $[P_1(A), P_2(A),...\ P_N(A)]$ which consist of the $A$ particles of the GHZ state. Upon receiving this $A$ particle sequence, they also perform a security check. If the security check is passed, they go to the next step.

Step 5: On Bob's side, when he receives the three blocks of particles step by step, he can make a GHZ state measurement on each of the GHZ-state and gets the state exactly as shown in equation (2) and thus gets the message which represent the message Alice sends.

Step 6: If the $N$ GHZ-states does not complete the task of communicating the secret message, then they continue with the next batch of $N$ GHZ-states, starting from step 1.

Under noisy channel, quantum error correction and privacy amplification have to be performed.

Compared to the two-particle Bell-basis state QSDC protocol, the three-particle GHZ state can transmit three bits of information each time though only two encoding unitary operations are performed on only two qubits, a characteristic signature of the superdense coding. When multi-partite entangled state are used, it will transmit more number of bits. The generalization of this scheme to multi-particle entangled states is given in the following. First Alice produces a squence of $N$ p-particle entangled states in the form

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0_1 0_2 ....0_p\rangle + |1_1 1_2 ....1_p\rangle). \quad (6)$$

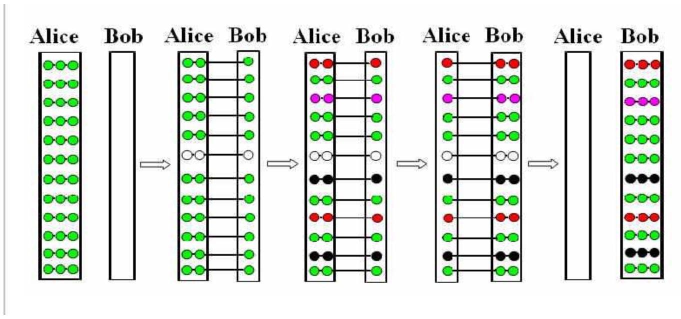


FIG. 1: The QSDC procedure using GHZ state.

The $p$th particle from each multiplet is sends to Bob first, and upon receiving this $p$th particle sequence, Alice and Bob perform security check so that they can assure the security of the channel. After assuring the security of the channel, Alice performs encoding operations on the remaining $p-1$ particles in each multiplet of particles: for the $(p-1)$th particle, four unitary operations are possible, namely $I$, $\sigma_x$, $i\sigma_y$ and $\sigma_z$, but for the remaining $p-2$ particles, only two unitary operations, $\sigma_x$ and $I$ are allowed. Though the unitary operations performed on only $p-1$ particles, the number of independent unitary operations is however $4 \times 2 \times \cdots \times 2 = 2^p$. Each time , a multiplet of entangled particles can transmit $p$ bits of classical information.

Another possible generalization of the scheme is to higher dimensions, namely qubit is generalized into qudit as in Ref. [18] in superdense coding. The maximally entangled GHZ- state in $d$-dimensional Hilbert space is

$$|\Psi_n\rangle = \frac{1}{\sqrt{d}} \sum_n |n\rangle_A \otimes |n\rangle_B \otimes |n\rangle_C \tag{7}$$

where $n = 0, 1, 2, ..., d-1$. The single particle unitary operations used for superdense coding are

$$U_{mn} = \sum_j e^{2\pi i j m/d} |j + n \bmod d\rangle\langle j|. \tag{8}$$

Using these unitary operations $U_{mn}$, one can construct superdense coding with $d$-dimensional single particle Hilbert space. To depict it explicitly, we formalize the multi-step superdense coding scheme in three-level Hilbert space. The three-level GHZ state is:

$$|\Psi_{00}\rangle_{ABC} = \frac{1}{\sqrt{3}}(|000\rangle_{ABC} + |111\rangle_{ABC} + |222\rangle_{ABC}). \tag{9}$$

By applying single qutrit unitary operations given in (8) with $d = 3$ on the first two particles $A$ and $B$ in the following combination, $U_{00}(A) \otimes U_{mn}(B)$, $U_{01}(A) \otimes U_{mn}(B)$, $U_{02}(A) \otimes U_{mn}(B)$, where $m, n \in 0, 1, 2$, one can make unique transformation from state (9) to any of the 27 independent three-qudits GHZ-state. For example,

$$\begin{aligned}
(U_{00} \otimes U_{mn})|\Psi_{00}\rangle &= \frac{1}{\sqrt{3}}(|0n0\rangle + e^{2m\pi i/3}|1(n+1 \bmod d)1\rangle \\
&\quad + e^{4m\pi i/3}|2(n+2 \bmod d)2\rangle), \\
(U_{01} \otimes U_{mn})|\Psi_{00}\rangle &= \frac{1}{\sqrt{3}}(|1n0\rangle + e^{2m\pi i/3}|2(n+1 \bmod d)1\rangle \\
&\quad + e^{4m\pi i/3}|0(n+2 \bmod d)2\rangle), \\
(U_{02} \otimes U_{mn})|\Psi_{00}\rangle &= \frac{1}{\sqrt{3}}(|2n0\rangle + e^{2m\pi i/3}|0(n+1 \bmod d)1\rangle \\
&\quad + e^{4m\pi i/3}|1(n+2 \bmod d)2\rangle).
\end{aligned} \tag{10}$$

Now we come to the multi-step QSDC using qudit superdense coding. In order to encode the secret message, Alice and Bob make an agreement on that each of the unitary operations $U_{00}(A) \otimes U_{mn}(B)$, $U_{01}(A) \otimes U_{mn}(B)$, $U_{02}(A) \otimes U_{mn}(B)$, where $m, n \in 0, 1, 2$, represent one number in the three ternary number such 000, 012 etc. Then the details of the protocol will be similar for the qubit GHZ-state case. The number of the possible unitary operations is $3^p$ which is a direct generalization of that with two-level quantum system, where $p$ is the number of particles.

It is worth emphasizing that the multi-step should not be replaced by a three-step process because it sacrifices the security. For instance, if we divide the $p-1$ particles into two parts with $p_1$ and $p_2$ each. First Alice sends Bob the last particle in each GHZ-state. Then she may perform the encoding operations on the remaining $p-1$ particles and send the $p_1$ first, and then later send the remaining $p_2$ particles after the security of the $p_1$ particles is assured. However, when Eve intercept those $p_1$ particles, she can obtain partial information. In the original GHZ-state, a measurement of the $p_1$ particles yields either $00\cdots0$ of $11\cdots1$, but after some unitary transformation, the measurement may obtain either $10\cdots1$ of $01\cdots0$. Eve may obtain partial information from such measurement. These partial information contains some secret message hence is risky. This is in striking contrast to quantum key distribution there the keys do not carry the secret message, one can simply drop the raw key if eavesdropping is discovered. By sending the particles in multi-steps, this danger is avoided since Eve's measurement on a single particle does not reveal any useful information.

The security of this multi-step QSDC with GHZ state is similar to that using EPR entangled states in Ref.[9]. When the entangled particles are not in one side, it is just like the BBM92 QKD protocol[2]. As the secret information is encoded in the whole entangled state, Eve can not get useful information if she just gets part of the entangled state. When Eve is in the quantum line, the state of the composite system is

$$|\psi\rangle = \sum_{a,b,c \in (0,1)} |\varepsilon\rangle |a, b\rangle |c\rangle \tag{11}$$

where $|\varepsilon\rangle$ is Eve's state used to probe the particle. $|a, b\rangle$ and $|c\rangle$ are GHZ states shared by Alice and Bob after the first step transmission. When she eavesdrops the $C$ particle sequence, the whole system will be:

$$\begin{aligned} |\psi\rangle =& \frac{1}{\sqrt{2}}[|00\rangle(\alpha_1|0\rangle|\varepsilon_{00}\rangle + \beta_1|1\rangle|\varepsilon_{01}\rangle) \\ &+ |11\rangle(\beta_2|1\rangle|\varepsilon_{10}\rangle + \alpha_2|0\rangle|\varepsilon_{11}\rangle)], \end{aligned} \tag{12}$$

where $\varepsilon_{00}$, $\varepsilon_{01}$, $\varepsilon_{10}$, $\varepsilon_{11}$ are Eve's states respectively. We can write out the probe operator

$$\widehat{E} = \begin{pmatrix} \alpha_1 & \beta_1 \\ \beta_2 & \alpha_2 \end{pmatrix}. \tag{13}$$

Because $\widehat{E}$ is an unitary operator, the complex number $\alpha_1$, $\alpha_2$, $\beta_1$, $\beta_2$ satisfy $|\alpha_1|^2 + |\beta_1|^2 = |\alpha_2|^2 + |\beta_2|^2 = 1$. The error rate introduced by Eve is $\epsilon = |\beta_1|^2 = |\beta_2|^2 = 1 - |\alpha_1|^2 = 1 - |\alpha_2|^2$. The security can thus be similarly analyzed.

The discussions above are based on the ideal conditions. If the channel noise cannot be omitted, the security problems arise. Eve may captures some of the particles in the sequence and send the left to Bob through a better channel. If she intercepts the message sequence, and does a GHZ-state measurement, she may gets some of the secret message. So there are probabilities of information leakage. To avoid the dangerous, we consider a entanglement swapping strategy. Bob perform the quantum entanglement swapping on the particles he receives and compare the result with Alice's: if the particles preserved there, the entanglement swapping succeed. They measures their particles with either $\sigma_z$ or $\sigma_x$. If they get the correlation results, the secure channel established and message sending can be protected.

In conclusion, we proposed the multi-step GHZ state quantum secure direct communication protocol and generalized it to the high dimensional qudit case. The security of the protocol is also discussed. In ideal condition, the protocol is safe against eavesdropping. In noisy channel, quantum privacy amplification has to be used to obtain security.

The authors wish to thank Drs Jian Wang,Quan Zhang, Lin-mei Liang, Chao-jing Tang for helpful discussions.

This work is supported the National Fundamental Research Program Grant No. 001CB309308, China National Natural Science Foundation Grant No. 60433005, the Hang-Tian Science Fund, and the Excellent Young University Teachers' Fund of Education Ministry of China.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* , 175-179, (IEEE, New Yoir, 1984).

[2] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[3] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[4] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **68**, 3121 (1992).

[5] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002), and the references therein.

[6] Y. S. Zhang, C. F. Li and G. C. Guo, Phys. Rev. A **64**, 024302 (2001); G. P. Guo, C.F. Li, B. S. Shi, J. Li and G. C. Guo, Phys. Rev. A **64**, 042301 (2001); P. Xue, C. F. Li, and G. C. Guo, Phys. Rev. A **65**, 022317 (2002).

[7] A. Beige, B.-G. Englert, C. Kurtsiefer, and H Weinfurter, Acta Phys. Pol. A **101**, 357 (2002); J. Phys. A **35**, L407 (2002).

[8] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).

[9] F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).

[10] F. G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).

[11] Q. Y. Cai and B. W. Li, Chin. Phys. Lett. **21**, 601 (2004).

[12] F. L. Yan and X. Zhang, Euro. Phys. Journal. B **41(1)**, 75 (2004).

[13] T. Gao, F. L. Yan and Z. X. Wang, NUOVE CIMENTO DELLA SOCIETA ITALIANA DI FISICA B **119** (3), 313 (2004).

[14] Z. J. Zhang, Z. X. Man an Y Li, Phys. Lett. A **333**, 46 (2004); Z. X. Man, Z. J. Zhang and Y. Li, Chin. Phys. Lett. **22**, 18 (2005).

[15] Q. Y. Cai and B. W. Li, Phys. Rev. A **69**,054301 (2004).

[16] T. Gao, F. L. Yan and Z. X. Wang, Zeitschrift fur Naturforschung A **59(9)**, 597 (2004).

[17] H. J. Lee, D. Ahn and S. W. Hwang, Phys. Rev. A **66**, 024304 (2004).

[18] X. S. Liu, G. L. Long, D. M. Tong and F. Li, Phys. Rev. A **65**, 022304 (2002).